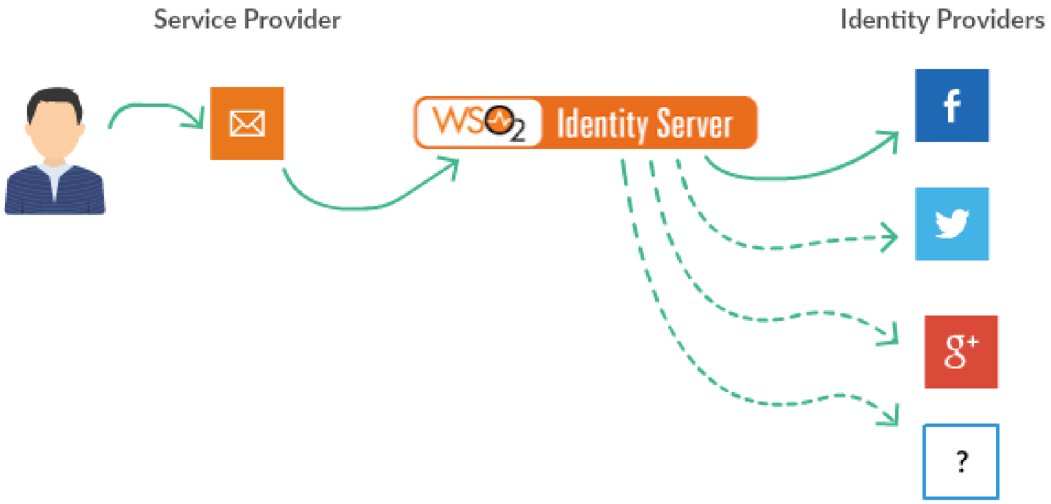
Federation

Introduction:

Identity federation is a mechanism that allows authentication across different enterprises in different trust domains based on a trust factor. This makes access easy, as users do not have to remember a different set of credentials for every application they use.

In this tutorial, we are going to see how to enable federated authentication with WSO2 Identity Server. Here we have used Google as the federated authenticator and a sample web application called pickup-dispatch for demonstration.

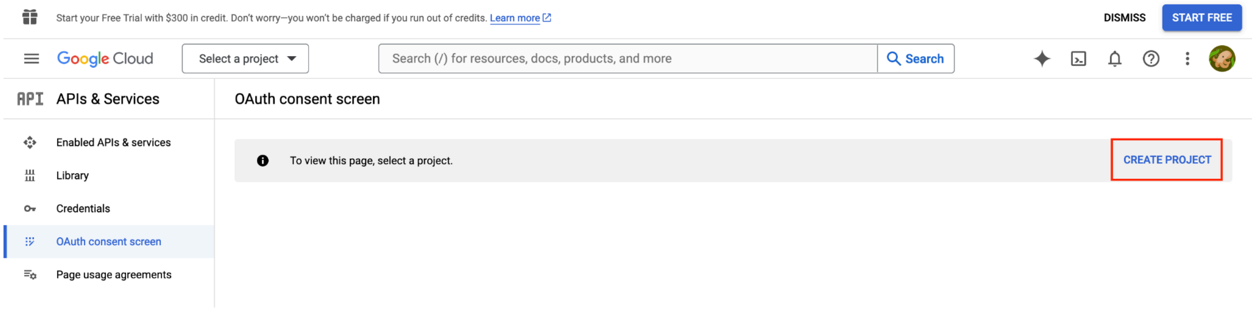
After successfully configuring Google as a federated authenticator, users will be able to authenticate by google credentials.



Setting up:

Configure Google Client Application

1. Go to Google API Console and navigate to the **Credentials** tab from the sidebar.
2. If you have not created a Project, create one using the option shown in the screen.

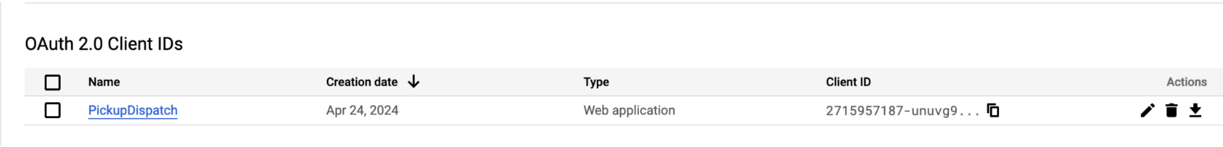


Start your Free Trial with $300 in credit. Don't worry—you won't be charged if you run out of credits. Learn more

To view this page, select a project.

3. Setup a consent screen if you have not already created one.
   a. Goto **OAuth consent screen** from the menu.
   b. Create **External** User Type Consent screen.
   c. Fill out the required fields and click **Save & Continue**.
   d. Keep the default configuration for the next two screens pops and click **Save & Continue**.
4. Then configure an OAuth web application in Google by selecting **OAuth Client ID** from the **Create Credentials** dropdown**.**
   a. Select **Web application** as the application type and give a name for the application (eg: PickupDispatch).

b. Enter the Authorized **redirect URI** as https://localhost:9443/commonauth (This is the endpoint in WSO2 Identity Server which accepts the response sent by Google).
c. Once the application client is created successfully, you will get the client ID and the client secret in a pop up screen.

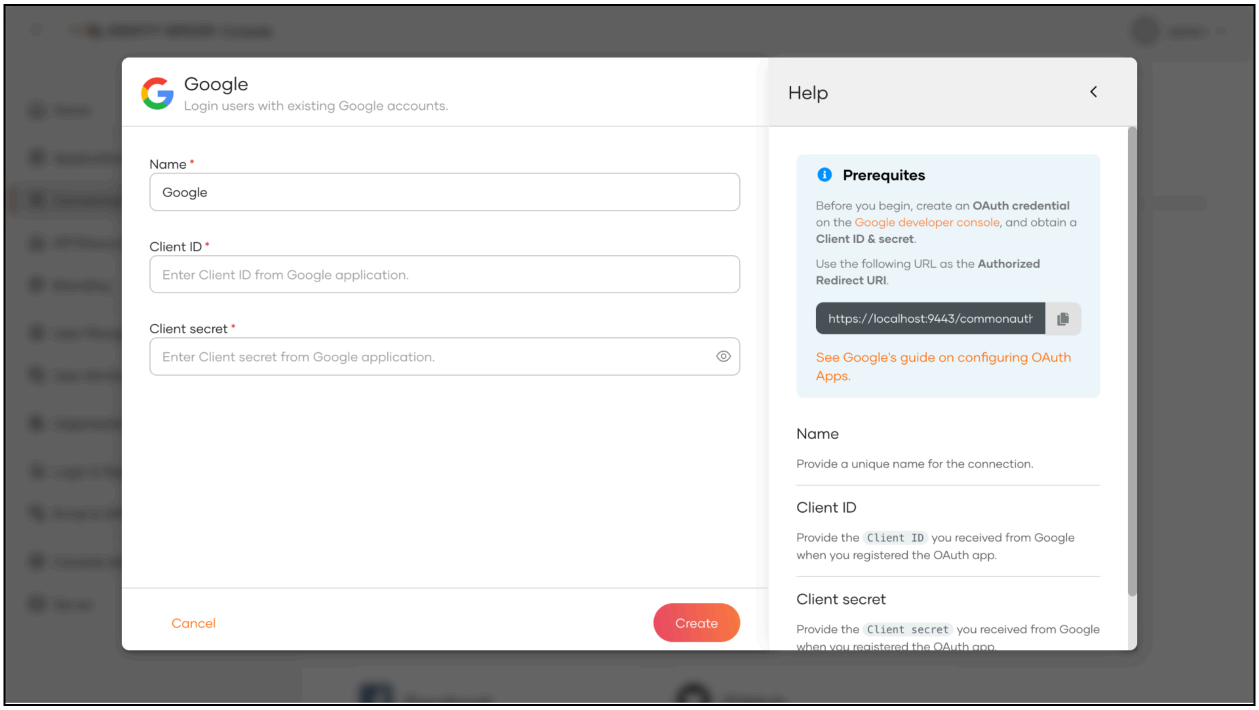


OAuth 2.0 Client IDs

□	Name	Creation date ↓	Type	Client ID	Actions
□	PickupDispatch	Apr 24, 2024	Web application	2715957187-unuvg9...	

Configure Google IdP in WSO2 IS

1. Login to the WSO2 Identity Server **Console,** using your admin credentials (e.g. admin:admin).
2. In the WSO2 Identity Server **Console,** from the menu click **Connections.**
3. Click + **New Connection**.
4. From the available templates select **Google** template.



Google
Login users with existing Google accounts.

Name *
Google

Client ID *
Enter Client ID from Google application.

Client secret *
Enter Client secret from Google application.

Prerequites

Before you begin, create an **OAuth credential** on the Google developer console, and obtain a **Client ID & secret**.

Use the following URL as the **Authorized Redirect URI**.

`https://localhost:9443/commonauth`

See Google's guide on configuring OAuth Apps.

Name

Provide a unique name for the connection.

Client ID

Provide the `Client ID` you received from Google when you registered the OAuth app.

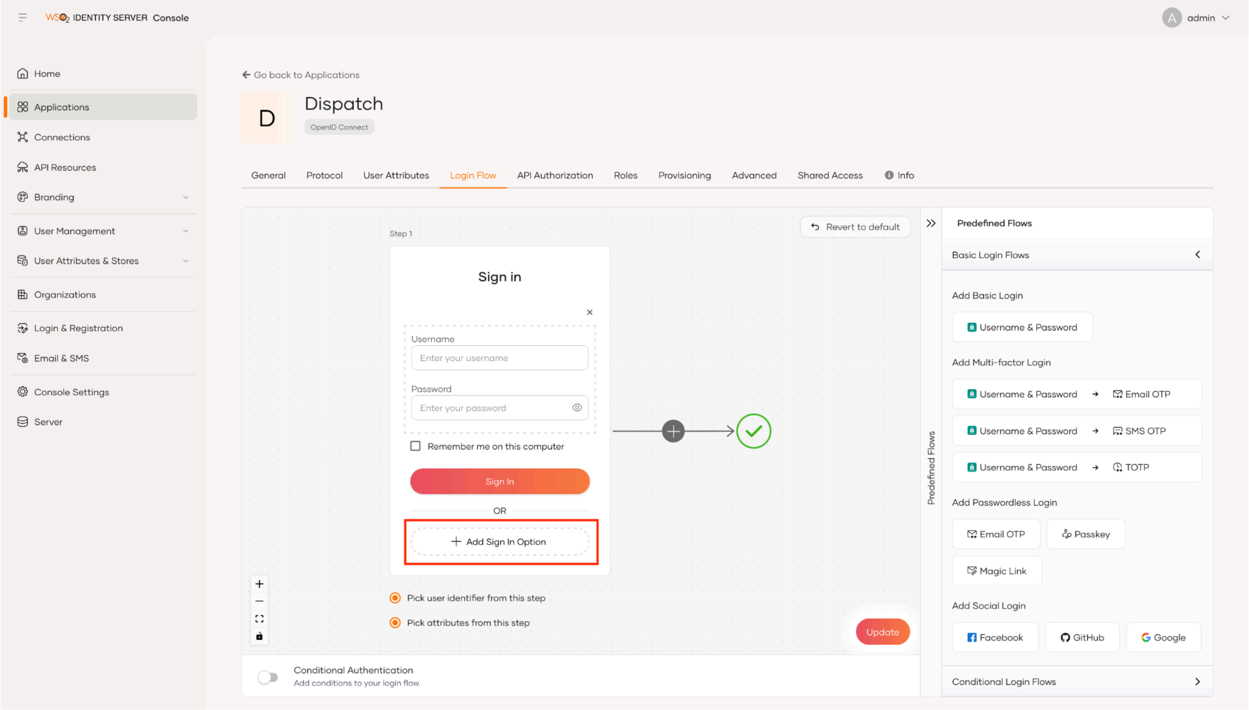
Client secret

Provide the `Client secret` you received from Google when you registered the OAuth app.

5. Add the noted **Client ID** and **Client Secret** extracted in Configure Google Client Application **step 6** in the respective fields.
6. Click **Create**.

Configure Login Flow in Sample Application

1. Use the **Dispatch** Application configured in **5. Single Sign-On with OpenID Connect** Lab.
2. In the WSO2 Identity Server **Console,** from the menu click **Applications.**
3. Click on application **Dispatch.**
4. Goto the Login Flow.
5. In the displayed mobile view click on the **+ Add Sign In Option**.



6. Scroll down a bit in the listed Authentication options.
7. Select **Google** and click **Add**.
8. Click **Update**.

Try It:

1. Open an Incognito Browser Window.
2. Access the link http://localhost.com:8080/pickup-dispatch and click on the **LOGIN** button.
3. You will be redirected to the **Google** Sign in page.
4. Provide the valid email credentials.
5. After providing the approval to view all the user information by clicking on the consent page, you will be logged into the **Dispatch** application.